Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1-28. *(Cancelled).*

29. *(Currently Amended)* A wireless database management system, comprising:

a first server providing a first virtual private network (VPN) and providing Internet access to client-held wireless communication appliances, the VPN limiting access to a subset of the wireless communication appliances that subscribe to the VPN; and

a second server providing a second VPN with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices;

wherein operation of the first VPN and second VPN creates a VPN tunnel in the Internet restricted to data addressed to or from the subscribing subset of wireless communication appliances[[.]]; and

wherein the wireless communication appliances include at least one of a personal digital assistant (PDA), cell phone, two-way pager or other mobile, hand-held, personal communication device.

30. *(Cancelled).*

31. *(Previously Presented)* The wireless database management system of claim 29 wherein the first virtual private network (VPN) operating on the first server providing Internet access to client-held wireless communication appliances is a VPN-controlled wireless proxy server securing data transferred between the client-held wireless communication appliances and the Internet.

32. *(Previously Presented)* The wireless database management system of claim 29, wherein the data transfers between the server providing Internet access to client-held wireless communication appliances are encrypted with a public key method.

33. *(Previously Presented)* The wireless database management system of claim 29, wherein the data transfers between the second server with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices are encrypted with a private key method.

34. *(Previously Presented)* The wireless database management system of claim 29, wherein users of the wireless communication appliances are authenticated before allowing access to the databases.

35. *(Previously Presented)* The wireless database management system of claim 29, wherein software is implemented on the second server with access to the Internet and providing access to one or more databases sets an adjustable timeout for connections between the wireless communication appliances and the server.

36. *(Previously Presented)* The wireless database management system of claim 35, wherein the second server identifies a session between the wireless communication appliances and the second server with a session identification phrase, and storing the session identification phrase in memory.

37. *(Previously Presented)* The wireless database management system of claim 29, wherein a firewall is implemented between the Internet and the second server connected to the databases, thereby limiting access to IP addresses of the wireless communication devices.

38. *(Previously Presented)* The wireless database management system of claim 37, wherein a second firewall is implemented between the second server and the databases.

39. *(Currently Amended)* A method for securing data transfers in a wireless database management system, comprising steps of:

(a) providing a first server including a virtual private network (VPN) and providing Internet access to client-held wireless communication appliances, the VPN limiting access to a subset of the wireless communication appliances that subscribe to the VPN; ~~and~~

(b) providing a second server including a VPN with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices; and

c) operating the first and second server VPNs to create a VPN tunnel in the Internet restricted to data addressed to or from the subscribing subset of wireless communication appliances[[.]];

wherein the wireless communication appliances include at least one of a personal digital assistant (PDA), cell phone, two-way pager or other mobile, hand-held, personal communication device.

40. *(Cancelled).*

41. *(Previously Presented)* The method of claim 39 wherein in step a), the first server providing Internet access to client-held wireless communication appliances is a VPN-controlled wireless proxy server securing data transferred between the client-held wireless communication appliances and the Internet.

42. *(Previously Presented)* The method of claim 39 wherein in step a) the data transfers between the first server providing Internet access to client-held wireless communication appliances are encrypted with a public key method.

43. *(Previously Presented)* The method of claim 39 wherein in step b) the data transfers between the second server with access to the Internet and providing access to one or more databases associated with the subscribing subset of wireless communication devices are encrypted with a private key method.

44. *(Previously Presented)* The method of claim 39, further providing a step of authenticating users of the wireless communication appliances before allowing access to the databases.

45. *(Previously Presented)* The method of claim 39 wherein in step b) an adjustable timeout is provided for connections between the wireless communication appliances and the second server.

46. *(Previously Presented)* The method of claim 39, further providing a step for identifying a session between the first server and the wireless communication appliances of step a) with a session identification phrase, and storing the session identification phrase in memory.

47. *(Previously Presented)* The method of claim 39 wherein in step b) a firewall is provided between the Internet and the second server connected to the databases, thereby limiting access to IP addresses of the wireless communication devices.

48. *(Previously Presented)* The method of claim 47 wherein a second firewall is implemented between the second server and the databases.